IN THE SPECIFICATION

Please replace the paragraph beginning at line 6, page 13 with the following rewritten paragraph:

FIG. 4 is more detailed diagram of circuits in embodiments of the present invention. A user (remote or local) may request a dialing action by entering a communication access number (e.g., a telephone number). This may be done by entering numbers on a keyboard 301, on a virtual dial pad on a display screen 302, voice recognition input (not shown) or by clicking a "hot spot" on display screen 302. The dialing action request would couple to dialing action controller ~~(DTC)~~ (DAC) 405 via system interface 412. The ~~DTC~~ DAC 405 would then signal to the user to input an authorization which may be entered via PIMs 409, 410 or 411. The device driver that actually does the dialing action is not stored in useable form within the IA, rather, the device driver (or necessary portions of the driver) are encrypted, using the security protocol, and stored as non-functional code. For example, the device driver code may be exclusively-ORed with a random pattern and this non-functional code may be then stored in the IA memory. The random pattern is a signed static message (or portion thereof) generated by a security protocol (e.g. the Public/Private key method explained above). In order to restore function, the device driver it must again be exclusively-ORed with the same random patter, which must be regenerated from a PIM prompt in the manner described above. The now functional device driver code may now be used to perform the dialing action. This method protects the code and therefore the dialing action in a manner that is not subject to brute force attack, due to the long length (typically 1024 bits) used in the Public/Private key crypto-system. Embodiments of the present invention employ a hardware security processor in the device to protect the Private keys and to do the Public/Private key cryptographic functions. Other embodiments may use software to implement the same mechanism with less protection for the Private keys. Embodiments of the present invention may obtain the PIM as described above using a hash of biometric data (e.g., fingerprint, retinal scan, etc.).

Please replace the paragraph beginning at line 10, page 14 with the following rewritten paragraph:

The entered PIM is then compared with a previously stored PIM (e.g., in RAM 314) within the security processor system. If the access is authorized, then the ~~DTC~~ DAC 405 sends appropriate signals over a Modem 406, 407 or 408 to establish a communication link. Incoming calls (with corresponding source numbers) received via Modems 406, 407 or 408 may be compared to stored numbers. These stored numbers may have been assigned responses such as; playing a pre-recorded message, recording the call (using answering or recording unit 412), or directing the call to another party via ~~DTC~~ DAC 405 and the IA 300. ~~DTC~~ DAC 405 may also send a connection cost alert to a user (e.g., display on 302) after an access has been authorized giving the user another option to either complete the connection or abort the dialing action request. The ~~DTC~~ DAC 405, via the system interface 412, may also employ security encryption for communication on an established link. For Internet telephony, a user may use a built-in key escrow function (e.g.,using the method previously described in pg. 10 line 20 to pg. 12 line 4) to notify a trusted server of a current Dynamic Host Configuration Protocol (DHCP) assigned Internet protocol (IP) address along with a "signature" indicating authenticity of transmission so that voice over IP services between devices and a web page server lookup may be performed in a DHCP environment without side-channel communication for call or web reference look-up.